UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JULIAN OLMEDA, individually and on behalf of all others similarly situated *Plaintiff*, v. THE VEGGIE GRILL, INC., a Delaware corporation, *Defendant.*	Case No. 20-cv-6982

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Julian Olmeda ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and Demand for Jury Trial against Defendant The Veggie Grill, Inc., for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1–99 ("BIPA"), and to obtain redress for persons injured by their conduct. Plaintiff alleges the following based on personal knowledge as to Plaintiff's own experiences, and as to all other matters, upon information and belief, including an investigation conducted by Plaintiff's attorneys.

INTRODUCTION

1. Defendant owns and operates a chain of vegan, fast-casual restaurants called Veggie Grill.

2. Veggie Grill currently has thirty-six locations nationwide, including four in Chicago.

3. Since 2008, Illinois has banned collection of people's biometric information or identifiers—for example, fingerprints, voiceprints, or faceprints—without their informed, written consent. 740 ILCS 14/15(b).

4. Despite the substantial privacy risks posed by the collection and storage of biometric data, and the decade-old prohibition on collecting and retaining biometric data in Illinois without informed consent, Defendant required its workers to use their fingerprints to clock in and out of shifts and breaks.

5. Defendant used the fingerprint scanners and timekeeping system (the "Biometric System") in its Chicago restaurant locations.

6. Defendant did not obtain informed, written consent to collect, retain, and disseminate workers' fingerprints and associated timekeeping data.

7. Defendant's scanning, retention, and disclosure of workers' fingerprints and associated timekeeping data is clearly unlawful in Illinois.

8. Plaintiff brings this Complaint seeking an order (i) declaring that Defendant's conduct violates BIPA, (ii) requiring that Defendant cease the unlawful activities described herein and destroy the biometric data it unlawfully collected, and (iii) awarding Plaintiff and the Class statutory damages of $1,000 for each negligent violation of BIPA and $5,000 for each violation found to be willful or reckless, plus their attorneys' fees and costs.

PARTIES

9. Plaintiff is a citizen of the State of Illinois and a resident of Cook County.

10. Defendant is a Delaware corporation with its headquarters and principal place of business located in Culver City, California. Defendant currently operates four restaurants in Chicago, Illinois.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendant because this lawsuit arises out of Defendant's conduct in Illinois.

12. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d)(2), because this is a class action in which Defendant is a citizen of different state than Plaintiff and other class members, and because the amount in controversy exceeds $5,000,000.00.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because Plaintiff resides in Cook County, which is within this District; because Plaintiff had his biometrics unlawfully collected from within this District; and because this lawsuit arises out of Defendant's conduct within this District.

COMMON FACTUAL ALLEGATIONS

The Biometric Information Privacy Act

14. Enacted in 2008, the Biometric Information Privacy Act regulates two types of biometric data. First, BIPA regulates any "biometric identifier," which means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. Second, it regulates "biometric information," which "means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

15. BIPA regulates the entire lifecycle of biometric data, from collection to use and disclosure.

16. As to collection, BIPA provides that "[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is

being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 714 ILCS 14/15(b).

17. Regarding disclosure, BIPA provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d).

18. Going a step further, BIPA prevents formation of a biometric-data market by decreeing without exception that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

19. To facilitate its notice-and-consent regime, BIPA also requires any private entity in possession of biometric identifiers or information to publish a written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

20. Finally, given the persistent nature of biometric data—one's fingerprints don't change—and the accompanying risks of misuse, BIPA requires any entity possessing biometric identifiers or information to "(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e).

21. To remedy the serious but difficult-to-quantify harms that accompany invasions of biometric privacy rights, BIPA creates a private right of action authorizing "[a]ny person aggrieved by a violation of" the statute to sue and recover for each unlawful scan liquidated damages of $1,000, or $5,000 in the event of an intentional or reckless violation, plus attorneys' fees, costs, and appropriate injunctive relief. 740 ILCS 14/20.

Defendant's Disregard for Workers' Privacy

22. Despite the recognized danger of using biometric data, Defendant used its employees' fingerprints to track their working hours.

23. Defendant did not inform its workers of the extent and purposes for which it collected their biometric data nor whether it ever disclosed that data to third parties.

24. Defendant also failed to maintain a written, publicly available policy identifying its biometric data retention schedule or providing guidelines for permanently destroying workers' fingerprints once they are no longer needed. Workers who left their jobs did so without any knowledge of when their biometric identifiers and information would be removed from Defendant's databases, if ever.

25. Workers using Defendants' Biometric System are likewise never told what might happen to their biometric data were Defendants or their employers to ever to go out of business.

26. Because Defendant neither published a BIPA-mandated data-retention policy nor disclosed the purposes for which it collected biometric data, workers were not told whether and how Defendant disclosed their biometric data, or what would happen to their biometric data were Defendant to be sold.

27. On top of its failure to notify workers and the public of the basics of their collection, use, retention, dissemination, and protection of biometric data, Defendant failed to obtain the written release required by BIPA before collecting workers' biometric data.

28. Defendant's failure to publish a biometric data-retention policy or obtain written releases from workers prior to the collection and dissemination of their fingerprints violated BIPA.

FACTS SPECIFIC TO PLAINTIFF

29. During the relevant time, Plaintiff worked for Defendant at its now-closed location at 614 West Diversey Avenue in Chicago.

30. While employing Plaintiff, Defendant used the Biometric System to monitor and manage its workers', including Plaintiff's, time on the job. To use the Biometric System, Plaintiff had to register a fingerprint, and scan the same finger each time he clocked in and out.

31. When Plaintiff became a shift leader, Plaintiff had to upload a different fingerprint and use that fingerprint to perform administrative functions such as new-user setup within the Biometric System.

32. Every time Plaintiff clocked in or out or set up a new user in the Biometric System, Defendant captured, collected, or otherwise obtained Plaintiff's biometric identifier in the form of his fingerprint.

33. Additionally, each time Plaintiff scanned his fingerprint into the Biometric System, biometric information was created which allowed Defendant to correctly attribute Plaintiff's work hours to his identity.

34. Defendant never informed Plaintiff of the specific purposes or length of time for which Defendant has collected, stored, and used Plaintiff's fingerprints.

35. Defendant did not obtain a written release authorizing the collection, capture, or subsequent disclosure of Plaintiff's biometric identifiers and information.

36. Defendant has not made publicly available any biometric data-retention policy, nor has Defendant informed Plaintiff whether it would ever permanently delete Plaintiff's fingerprints and the associated biometric information.

37. Further, on information and belief, Defendant disseminated information derived from the scanning of Plaintiff's biometric identifiers to third parties, including vendors for timekeeping, data storage, and payroll purposes.

38. Plaintiff has continuously and repeatedly been exposed to the harms and risks created by Defendant's violations of BIPA.

39. By failing to comply with BIPA, Defendant has violated Plaintiff's privacy rights.

CLASS ALLEGATIONS

40. Plaintiff brings this case as a class action under Fed. R. Civ. P. 23(b)(3). Plaintiff seeks to represent a Class defined as follows: All individuals who used Defendant's Biometric System within the State of Illinois.

41. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officers or directors.

42. **Numerosity:** Upon information and belief, there are scores, if not hundreds, of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be easily identified through Defendant's personnel records.

43. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class Plaintiff seeks to represent, because the factual and legal bases of Defendant's liability to Plaintiff and the other members are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the Class have all suffered damages as a result of Defendant's BIPA violations.

44. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant's conduct is subject to BIPA;

b. Whether Defendant made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics;

c. Whether Defendant obtained a written release from the Class before capturing, collecting, or otherwise obtaining their biometrics;

d. Whether Defendant provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used before taking such biometrics;

e. Whether Defendant's conduct violates BIPA;

f. Whether Defendant's violations of the BIPA are willful or reckless; and

g. Whether Plaintiff and the Class are entitled to damages and injunctive relief.

45. **Superiority:** Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy.

The class treatment of common questions of law and fact is superior to multiple individual actions in that it conserves the resources of the courts and the litigants and promotes consistency of adjudication.

46. **Adequacy:** Plaintiff will adequately represent and protect the interests of the members of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor Plaintiff's counsel have any interest adverse to those of the other members of the Class.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/15
On Behalf of Plaintiff and the Class

47. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

48. Defendant is a Delaware corporation, and is therefore a "private entity" under 740 ILCS 14/10.

49. Every time Plaintiff and the Class members used Defendant's Biometric System, Defendant obtained a scan of their fingerprints. Those fingerprint scans were used to produce information that identified Plaintiff and the Class members and tied them to particular timekeeping records. Defendants therefore collected, captured, received through trade, or otherwise obtained Plaintiff's and the Class members' biometric identifiers and biometric information. 740 ILCS 14/10.

50. On information and belief, Defendant disseminated information derived from the scanning of Plaintiff's biometric identifiers to third parties, including vendors for timekeeping, data storage, and payroll purposes.

51. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiff's and the Class members' biometric identifiers and biometric information, Defendant did not inform Plaintiff or the Class members or their legally authorized representatives that their biometric identifiers and information would be collected or stored. 740 ILCS 14/15(b)(1).

52. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiff's and the Class members' biometric identifiers and biometric information, Defendant did not inform Plaintiff or the Class members or their legally authorized representatives of the specific purpose and length of time for which their biometric identifiers and information were being collected, stored, and used. 740 ILCS 14/15(b)(2).

53. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiff's and the Class members' biometric identifiers and biometric information, Defendant did not receive a written release from Plaintiff and the Class members or their legally authorized representatives authorizing the collection, capture, receipt through trade, or other obtainment and use of their biometric identifiers or information. 740 ILCS 14/15(b)(3).

54. Prior to disclosing Plaintiff's and the Class members' biometric identifiers and biometric information, Defendant did not obtain consent to the disclosure from Plaintiff and the Class or their legally authorized representatives, nor was Defendant otherwise lawfully authorized to disclose Plaintiff's and the Class's biometrics.

55. Despite collecting and disclosing Plaintiff's and the Class members' biometric identifiers and biometric information, Defendant failed and continues to fail to maintain a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years

of the individual's last interaction with the private entity, whichever comes first. 740 ILCS 14/15(a).

56. By capturing and collecting, storing, using, and disclosing Plaintiff's and the Class members' biometric identifiers and information as described herein, Defendant violated Plaintiff's and the Class members' rights to privacy and property in their biometric data.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that this Court enter an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing Plaintiff's lawyers as Class Counsel;

B. Declaring that Defendant's actions, as described above, violate 740 ILCS 14/15;

C. Awarding liquidated damages under 740 ILCS 14/20 of $1,000 for each negligent violation of BIPA and $5,000 for each violation found to be willful or reckless;

D. Awarding injunctive and other equitable relief as necessary to protect the Class, including an order requiring Defendant to stop its unlawful collection of biometric data and to delete any such data that was unlawfully obtained;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: November 24, 2020

Respectfully submitted,

Julian Olmeda, individually and on behalf of a class of similarly situated individuals

By: /s/ Thomas R. Kayes
One of Plaintiff's Attorneys

Thomas R. Kayes
LAW OFFICES OF THOMAS R. KAYES, LLC
2045 W. Grand Ave. Suite B, PMB 62448
Chicago, IL 60612
Tel: (708) 722-2241
tom@kayes.law

Counsel for Plaintiff and the Putative Class